Title: **SYSTEM AND METHOD FOR ENCODING INFORMATION IN MAGNETIC STRIPE FORMAT FOR USE IN RADIO FREQUENCY IDENTIFICATION TRANSACTIONS**

Inventor: **Michael J. Berardi, Ft. Lauderdale, Florida**
Michal Bliman, Matawan, New Jersey
David S. Bonalle, New Rochelle, New York
Peter D. Saunders, Salt Lake City, Utah

Assignee: **American Express Travel Related Systems Company, Inc.**

Related Applications

This invention is a continuation in part of, and claims priority to U.S. Patent Application No. 10/192,488, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed on July 9, 2002 (which itself claims priority to U.S. Provisional Patent Application No. 60/304,216, filed July 10, 2001), and to U.S. Patent Application No. 10/340,352, entitled "SYSTEM AND METHOD FOR INCENTING PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed January 10, 2003 (which itself claims priority to U.S. Provisional Patent Application No. 60/396,577, filed July 16, 2002), all of which are incorporated herein by reference.

Field of Invention

[0001] This invention generally relates to a system and method for completing a transaction, and more particularly, to completing a transaction using a proxy transaction account identifier which emulates a transaction account number in a merchant recognizable format.

Background of the Invention

[0002] Like barcode and voice data entry, RFID is a contactless information acquisition technology. RFID systems are wireless, and are usually extremely effective in hostile environments where conventional acquisition methods fail. RFID has established itself in a wide range of markets, such as, for example, the high-speed reading of railway containers, tracking moving objects such as livestock or automobiles, and retail inventory applications. As such, RFID technology has become a primary focus in automated data collection, identification and analysis systems worldwide.

[0003] Of late, companies are increasingly embodying RFID data acquisition technology in a fob or tag for use in completing financial transactions. A typical fob includes a transponder and is ordinarily a self-contained device which may be contained on any portable form factor. In some instances, a battery may be included with the fob to power the transponder. In which case the internal circuitry of the fob (including the transponder) may draw its operating power from the battery power source. Alternatively, the fob may exist independent of an internal power source. In this instance the internal circuitry of the fob (including the transponder) may gain its operating power directly from an RF interrogation signal. U.S. Patent No. 5,053,774 issued to Schuermann describes a typical transponder RF interrogation system which may be found in the prior art. The Schuermann patent describes in general the powering technology surrounding conventional transponder structures. U.S. Patent No. 4,739,328 discusses a method by which a conventional transponder may respond to a RF interrogation signal. Other typical modulation techniques which may be used include, for example, ISO/IEC 14443 and the like.

[0004] In the conventional fob systems, the fob is provided a fob identifier. The fob may be activated or powered upon presenting the fob in an interrogation signal provided by a fob reader. Once the transaction device is interrogated, the

transponder included in the fob may provide the fob identifier to an authorizing entity who may correlate the fob identifier to a customer account number which is recognizable by a merchant system. That is, the information stored on the traditional fob ordinarily must be translated by an authorizing entity in order for the merchant system to be able to process the transaction request.

[0005] The customer account number may be stored on an authorizing entity database. An authorizing entity server may receive the fob identifier and correlate the fob identifier to a customer account number, which is ordinarily maintained in the authorizing entity's system database. Since the customer account number is typically a conventional credit, debit or loyalty account number, the fob may be presented to complete a transaction whereby the authorizing agent translates the fob identifier to a customer account number and provides the customer account number to the merchant system for processing under business as usual standards. The merchant system ordinarily provides the customer account number to a customer account provider which uses the number to locate the corresponding transaction account to be used to satisfy the customer's transaction request.

[0006] One of the more visible uses of the RFID technology is found in the introduction of Exxon/Mobil's Speedpass® and Shell's EasyPay® products. These products use transponders placed in a fob or tag which enables automatic identification of the user when the fob is presented at a Point of Sale (POS) device. Fob identification data is typically passed to a third-party server database, where the identification data is referenced or translated into a customer (*e.g.*, user) credit or debit account. In an exemplary processing method, the third-party server seeks authorization for the transaction by passing a transaction request and account data to an authorizing entity. Once authorization is received by the server, clearance is sent to the point of sale device for completion of the transaction. In this way, the conventional transaction processing method involves an indirect path which causes

undue overhead due to the use of the third-party server to correlate the fob identification data to a customer account prior to providing the accompanying transaction request to the merchant POS for completion.

[0007] A need exists for a transaction authorization system which allows fob transactions to be authorized while eliminating the cost associated with using third-party servers.

Summary of the Invention

[0008] Described herein is a system and method for securing a transaction using a proxy transaction account identifier stored in the database of a transaction device. The proxy transaction account identifier may be segmented into multiple portions used to provide to a transaction account provider data corresponding to the a customer transaction account. The customer transaction account may include various data relevant to the account or the accountholder. For example, the customer transaction account data may include such data as the account expiration date, account identifier, account provider routing number, authentication tag, secondary security code (*e.g.*, Personal Identification Number), effective date, and the like as is commonly found. At least one of the multiple portions of the proxy transaction account identifier may have portions of a merchant recognizable customer transaction account data stored therein.

[0009] The portions of the transaction account data included in the proxy transaction account identifier may be encrypted. The account data may be encrypted using a cryptogram generated by the transaction device to which the proxy transaction account identifier is associated. The transaction device may calculate a complete cryptogram using changing values from the transaction device and data received from a point of sale device (POS) linked to a merchant system. Once the transaction device calculates the cryptogram and encrypts the various portions of

account data, the encrypted account data and a portion of the cryptogram may then be sent to the transaction account provider as a part of at least one of the multiple portions of the proxy account identifier. In this way, the space requirements for sending the proxy transaction device information is reduced.

[0010] The transaction account provider receives the proxy account identifier and recalculates the cryptogram using the encrypted account identifier data. The account provider may then verify the portion of the cryptogram included in the proxy account identifier, by for example comparing the portion of the cryptogram with the recalculated cryptogram to determine if a match exists. The account provider may decrypt the portions of the proxy account identifier and locate the corresponding account using the portions of the transaction account data. For example, the portions of the transaction account data may be subjected to an account provider defined algorithm used to generate the complete transaction account data from the portions of the account data provided in the proxy account identifier.

[0011] The proxy account identifier may take the form of any suitable data transmission which is recognizable by the merchant system. That is, the merchant system does not detect that the proxy account identifier includes only partial account information. This is true because the invention includes the partial account information in any traditional account information format. For example, if the merchant system is configured to receive information in magnetic stripe format, the proxy account identifier is provided to the merchant system in magnetic stripe format. As such, the present invention is more advantageous than conventional fob devices in that the proxy transaction account identifier does not have to be sent to a third-party authorizing entity for correlation to a customer number formatted in magnetic stripe which may then be sent to a merchant system for processing. The present invention eliminates the cost associated with involving a third-party server to

translate the account fob data into a merchant recognizable format (*e.g.*, magnetic stripe).

[0012] In addition, the transaction device according to the present invention may include a transponder system for using RFID technology to initiate and complete financial transactions. The transaction system described herein may include a RFID reader operable to provide a RF interrogation signal for powering a transponder system, receiving a transponder system RF signal, and providing proxy account identifier account data relative to the transponder system RF signal. The transponder-reader payment system may include a RFID protocol/sequence controller in electrical communication with one or more interrogators for providing an interrogation signal to a transponder, and a RFID authentication circuit for authenticating the signal received from the transponder. The transponder-reader payment system may further include a fob including one or more transponders (*e.g.*, modules) responsive to the interrogation signal and for providing an authentication signal for verifying that the transponder and/or the RFID reader are authorized to operate within the transponder-reader payment system. In this way, the transponder may be responsive to multiple interrogation signals provided at different frequencies. Further, the transponder may include a USB or serial interface for use with a computer network or with the RFID reader.

[0013] The RFID system and method according to the present invention may include a RFID-ready terminal and a transponder which may be embodied in a transaction device taking any suitable form capable of being presented for interrogation, such as, a fob, tag, card or any other form factor (*e.g.*, wristwatch, keychain, cell phone, etc.), or the like. In that regard, although the transaction device is described herein as embodied in a fob, the invention is not so limited.

[0014] The system may further include a RFID reader configured to send a standing RFID recognition signal which may be transmitted from the RFID reader via radio

frequency (or electromagnetic) propagation. The fob may be placed within proximity to the RFID reader such that the RFID signal may interrogate the fob and initialize fob identification procedures.

[0015] These features and other advantages of the system and method, as well as the structure and operation of various exemplary embodiments of the system and method, are described below.

Brief Description of the Drawings

[0016] The accompanying drawings, wherein like numerals depict like elements, illustrate exemplary embodiments of the present invention, and together with the description, serve to explain the principles of the invention. In the drawings:

[0017] FIG. 1 illustrates an exemplary RFID-based system in accordance with the present invention, wherein exemplary components used for fob transaction completion are depicted;

[0018] FIG. 2 is a schematic illustration of an exemplary transponder system in accordance with the present invention;

[0019] FIG. 3 is a schematic illustration of an exemplary RFID reader in accordance with the present invention;

[0020] FIG. 4 is an exemplary flow diagram of an exemplary authentication process in accordance with the present invention;

[0021] FIG. 5 is an exemplary flow diagram of an exemplary decision process for a protocol/sequence controller in accordance with the present invention;

[0022] FIG. 6 is a flow diagram of an exemplary payment/transaction process in accordance with the present invention;

[0023] FIG. 7 illustrates an exemplary layout of data fields for encoding data in traditional magnetic stripe track 1;

[0024] FIG. 8 illustrates an exemplary layout of data fields for encoding data in traditional magnetic stripe track 2;

[0025] FIG. 9 illustrates an exemplary layout of proxy fields for encoding data in proxy track 1 format;

[0026] FIG. 10 illustrates an exemplary layout of proxy fields for encoding data in proxy track 2 format;

[0027] FIG. 11 is an illustration of an exemplary proxy transaction account identifier transaction, in accordance with an exemplary embodiment of the present invention;

[0028] FIG. 12 is an example of a conventional magnetic stripe track 2 layout for MasterCard; and

[0029] FIG. 13 is an example of a proxy track 2 layout for MasterCard in accordance with the present invention.

Detailed Description

[0030] The present invention may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. Such functional blocks may be realized by any number of hardware and/or software components configured to perform to specified functions. For example, the present invention may employ various integrated circuit components (*e.g.*, memory elements, processing elements, logic elements, look-up tables, and the like), which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language or platforms such as C, C++, Java, JavaCard applets, MULTOS Executive Language, COBOL, assembler, PERL, extensible markup language (XML), JavaCard and MULTOS with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming

elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. For a basic introduction on cryptography, review a text written by Bruce Schneier entitled "Applied Cryptography: Protocols, Algorithms, and Source Code in C," published by John Wiley & Sons (second edition, 1996), herein incorporated by reference.

[0031] In addition, many applications of the present invention could be formulated. The exemplary network disclosed herein may include any system for exchanging data or transacting business, such as the internet, an intranet, an extranet, WAN, LAN, satellite communications, and/or the like. It is noted that the network may be implemented as other types of networks, such as an interactive television network (ITN).

[0032] Where required, the system user may interact with the system via any input device such as, a keypad, keyboard, mouse, kiosk, personal digital assistant, handheld computer (*e.g.*, Palm Pilot®, Blueberry®), cellular phone and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, work station, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, Solaris or the like. Moreover, although the invention may frequently be described as being implemented with TCP/IP communications protocol, it should be understood that the invention could also be implemented using SNA, IPX, Appletalk, IPte, NetBIOS, OSI or any number of communications protocols. Moreover, the system contemplates, the use, sale, or distribution of any goods, services or information over any network having similar functionality described herein.

[0033] FIG. 1 illustrates an exemplary RFID transaction system 100 in accordance with the present invention, wherein exemplary components for use in completing a

fob transaction are depicted. In general, the operation of system 100 may begin when fob transponder system 102 (*e.g.*, fob 102) is presented for payment, and is interrogated by RFID reader 104 or, alternatively, interface 134. Fob 102 and RFID reader 104 may then engage in mutual authentication after which the transponder 102 may provide the transponder identification and/or account identifier to the RFID reader 104 which may further provide the information to the merchant system 130 POS device 110.

[0034] System 100 may include a fob 102 having a transponder 114 and a RFID reader 104 in RF communication with fob 102. Although the present invention is described with respect to a fob 102, the invention is not to be so limited. Indeed, system 100 may include any transaction device configured to communicate data for transaction completion. In one exemplary embodiment the transaction device may be configured to communicate with a RFID reader 104 via RF communication. Typical devices may include, for example, a key ring, tag, card, cell phone, wristwatch or any such form capable of being presented for interrogation.

[0035] The RFID reader 104 may be configured to communicate using a RFID internal antenna 106. Alternatively, RFID reader 104 may include an external antenna 108 for communications with fob 102, where the external antenna may be made remote to the RFID reader 104 using a suitable cable and/or data link 120. RFID reader 104 may be further in communication with a merchant system 130 via a data link 122. The system 100 may include a transaction completion system including a point of interaction device such as, for example, a merchant point of sale (POS) device 110 or a computer interface (*e.g.*, user interface) 134. In one exemplary embodiment the transaction completion system may include a merchant system 130 including the POS device 110 in communication with a RFID reader 104 (via data link 122). As described more fully below, the transaction completion

system may include the user interface 134 connected to a network 136 and to the transponder via a USB connector 132.

[0036] Although the point of interaction device is described herein with respect to a merchant point of sale (POS) device, the invention is not to be so limited. Indeed, a merchant POS device is used herein by way of example, and the point of interaction device may be any device capable of receiving data relative to fob 102. In this regard, the POS device 110 may be any point of interaction device enabling the user to complete a transaction using a fob 102. POS device 110 may be in further communication with a customer interface 118 (via data link 128) for entering at least a customer identity verification information. In addition, POS device 110 may be in communication with a merchant host network 112 (via data link 124) for processing any transaction request. In this arrangement, information provided by RFID reader 104 is provided to the POS device 110 of merchant system 130 via data link 122. The POS device 110 may receive the information (and alternatively may receive any identity verifying information from customer interface 118 via data link 128) and provide the information to host system 112 for processing.

[0037] A variety of conventional communications media and protocols may be used for data links 120, 122, 124, and 128. For example, data links 120, 122, 124, and 128 may be an Internet Service Provider (ISP) configured to facilitate communications over a local loop as is typically used in connection with standard modem communication, cable modem, dish networks, ISDN, Digital Subscriber Lines (DSL), or any wireless communication media. In addition, the merchant system 130 including the POS device 110 and host network 112 may reside on a local area network which interfaces to a remote network (not shown) for remote authorization of an intended transaction. The merchant system 130 may communicate with the remote network via a leased line, such as a T1, D3 line, or the like. Such communications lines are described in a variety of texts, such as,

"Understanding Data Communications," by Gilbert Held, which is incorporated herein by reference.

[0038] An account number, as used herein, may include any identifier for an account (*e.g.*, credit, charge debit, checking, savings, reward, loyalty, or the like) which may be maintained by a transaction account provider (*e.g.*, payment authorization center) and which may be used to complete a financial transaction. A typical account number (*e.g.*, account data) may be correlated to a credit or debit account, loyalty account, or rewards account maintained and serviced by such entities as American Express, Visa and/or MasterCard or the like. For ease in understanding, the present invention may be described with respect to a credit account. However, it should be noted that the invention is not so limited and other accounts permitting an exchange of goods and services for an account data value is contemplated to be within the scope of the present invention.

[0039] In addition, the account number (*e.g.*, account data) may be associated with any device, code, or other identifier/indicia suitably configured to allow the consumer to interact or communicate with the system, such as, for example, authorization/access code, personal identification number (PIN), Internet code, digital certificate, biometric data, and/or other identification indicia. The account number may be optionally located on a rewards card, charge card, credit card, debit card, prepaid card, telephone card, smart card, magnetic stripe card, bar code card, and/or the like. The account number may be distributed and stored in any form of plastic, electronic, magnetic, and/or optical device capable of transmitting or downloading data to a second device. A customer account number may be, for example, a sixteen-digit credit card number, although each credit provider has its own numbering system, such as the fifteen-digit numbering system used by American Express. Each company's credit card numbers comply with that company's standardized format such that the company using a sixteen-digit format

will generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". Additionally, the first five to seven digits may be reserved for processing purposes and identify the issuing bank, card type and etc. In a typical example, the first digit of the account number may be a common character which may correspond to a particular account provider. For example, account numbers beginning with the common character 4 may correspond to transaction accounts provided by VISA; account numbers beginning with the number 5 may correspond to transaction accounts provided by MASTERCARD; account numbers beginning with the common character 3 may correspond to transaction accounts provided by AMERICAN EXPRESS. In this example, the last sixteenth digit, sometimes called the "Longitudinal Redundancy Check" character, is used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer.

[0040] The account number may be stored as Track 1 and Track 2 data as defined in ISO/IEC 7813, and further may be made unique to fob 102. In one exemplary embodiment, the account number may include a unique fob serial number and user identification number, as well as specific application applets. The account number may be stored in fob 102 inside a database 214, as described more fully below. Database 214 may be configured to store multiple account numbers issued to the fob 102 user by the same or different account providing institutions. Where the account data corresponds to a loyalty or rewards account, the database 214 may be configured to store the attendant loyalty or rewards points data.

[0041] FIG. 2 illustrates a block diagram of the many functional blocks of an exemplary fob 102 in accordance with the present invention. Fob 102 may be a RFID fob 102 which may be presented by the user to facilitate an exchange of funds or points, etc., for receipt of goods or services. As described herein, by way of

example, the fob 102 may be a RFID fob which may be presented for facilitating payment for goods and/or services.

[0042] Fob 102 may include an antenna 202 for receiving an interrogation signal from RFID reader 104 via antenna 106 (or alternatively, via external antenna 108). Fob antenna 202 may be in communication with a transponder 114. In one exemplary embodiment, transponder 114 may be a 13.56 MHz transponder compliant with the ISO/IEC 14443 standard, and antenna 202 may be of the 13 MHz variety. The transponder 114 may be in communication with a transponder compatible modulator/demodulator 206 configured to receive the signal from transponder 114 and configured to modulate the signal into a format readable by any later connected circuitry. Further, modulator/demodulator 206 may be configured to format (*e.g.*, demodulate) a signal received from the later connected circuitry in a format compatible with transponder 114 for transmitting to RFID reader 104 via antenna 202. For example, where transponder 114 is of the 13.56 MHz variety, modulator/demodulator 206 may be ISO/IEC 14443-2 compliant.

[0043] Modulator/demodulator 206 may be coupled to a protocol/sequence controller 208 for facilitating control of the authentication of the signal provided by RFID reader 104, and for facilitating control of the sending of the fob 102 account number. In this regard, protocol/sequence controller 208 may be any suitable digital or logic driven circuitry capable of facilitating determination of the sequence of operation for the fob 102 inner-circuitry. For example, protocol/sequence controller 208 may be configured to determine whether the signal provided by the RFID reader 104 is authenticated, and thereby providing to the RFID reader 104 the account number stored on fob 102.

[0044] Protocol/sequence controller 208 may be further in communication with authentication circuitry 210 for facilitating authentication of the signal provided by RFID reader 104. Authentication circuitry may be further in communication with a

non-volatile secure memory database 212. Secure memory database 212 may be any suitable elementary file system such as that defined by ISO/IEC 7816-4 or any other elementary file system allowing a lookup of data to be interpreted by the application on the chip. Database 212 may be any type of database, such as relational, hierarchical, object-oriented, and/or the like. Common database products that may be used to implement the databases include DB2 by IBM (White Plains, New York), any of the database products available from Oracle Corporation (Redwood Shores, California), Microsoft Access or MSSQL by Microsoft Corporation (Redmond, Washington), or any other database product. Database 212 may be organized in any suitable manner, including as data tables or lookup tables. Association of certain data may be accomplished through any data association technique known and practiced in the art. For example, the association may be accomplished either manually or automatically. Automatic association techniques may include, for example, a database search, a database merge, GREP, AGREP, SQL, and/or the like. The association step may be accomplished by a database merge function, for example, using a "key field" in each of the manufacturer and retailer data tables. A "key field" partitions the database according to the high-level class of objects defined by the key field. For example, a certain class may be designated as a key field in both the first data table and the second data table, and the two data tables may then be merged on the basis of the class data in the key field. In this embodiment, the data corresponding to the key field in each of the merged data tables is preferably the same. However, data tables having similar, though not identical, data in the key fields may also be merged by using AGREP, for example.

[0045] The data may be used by protocol/sequence controller 208 for data analysis and used for management and control purposes, as well as security purposes. Authentication circuitry may authenticate the signal provided by RFID reader 104 by

association of the RFID signal to authentication keys stored on database 212. Encryption circuitry may use keys stored on database 212 to perform encryption and/or decryption of signals sent to or from the RFID reader 104.

[0046] In addition, protocol/sequence controller 208 may be in communication with a database 214 for storing at least a fob 102 account data, and a unique fob 102 identification code. Protocol/sequence controller 208 may be configured to retrieve the account number from database 214 as desired. Database 214 may be of the same configuration as database 212 described above. The fob account data and/or unique fob identification code stored on database 214 may be encrypted prior to storage. Thus, where protocol/sequence controller 208 retrieves the account data, and or unique fob identification code from database 214, the account number may be encrypted when being provided to RFID reader 104. Further, the data stored on database 214 may include, for example, an unencrypted unique fob 102 identification code, a user identification, Track 1 and 2 data, as well as specific application applets.

[0047] Fob 102 may be configured to respond to multiple interrogation frequency transmissions provided by RFID reader 104. That is, as described more fully below, RFID reader 104 may provide more than one RF interrogation signal. In this case, fob 102 may be configured to respond to the multiple frequencies by including in fob 102 one or more additional RF signal receiving/transmitting units 226. RF signal receiving/transmitting unit 226 may include an antenna 218 and transponder 220 where the antenna 218 and transponder 220 are compatible with at least one of the additional RF signals provided by RFID reader 104. For example, in one exemplary embodiment, fob 102 may include a 134 KHz antenna 218 configured to communicate with a 134 KHz transponder 220. In this exemplary configuration, an ISO/IEC 14443-2 compliant modulator/demodulator may not be required. Instead, the 134 KHz transponder may be configured to communicate directly with the

protocol/sequence controller 208 for transmission and receipt of authentication and account number signals as described above.

[0048] In another embodiment, fob 102 may further include a universal serial bus (USB) connector 132 for interfacing fob 102 to a user interface 134. User interface 134 may be further in communication with a POS device 110 via a network 136. Network 136 may be the Internet, an intranet, or the like as is described above with respect to network 112. Further, the user interface 134 may be similar in construction to any conventional input devices and/or computing systems aforementioned for permitting the system user to interact with the system. In one exemplary embodiment, fob 102 may be configured to facilitate online Internet payments. A USB converter 222 may be in communication with a USB connector 232 for facilitating the transfer of information between the modulator/demodulator 206 and USB connector 132. Alternatively, USB converter 222 may be in communication with protocol/sequence controller 208 to facilitate the transfer of information between protocol/sequence controller 208 and USB connector 132.

[0049] Where fob 102 includes a USB connector 132, fob 102 may be in communication with, for example, a USB port on user interface 134. The information retrieved from fob 102 may be compatible with credit card and/or smart card technology enabling usage of interactive applications on the Internet. No RFID reader may be required in this embodiment since the connection to POS device 110 may be made using a USB port on user interface 134 and a network 136.

[0050] Fob 102 may include means for enabling activation of the fob by the user. In one exemplary embodiment, a switch 230 which may be operated by the user of the fob 102. The switch 230 on fob 102 may be used to selectively or inclusively activate the fob 102 for particular uses. In this context, the term "selectively" may mean that the switch 230 enables the user to place the fob 102 in a particular operational mode. For example, the user may place the fob 102 in a mode for

enabling purchase of a good or of a service using a selected account number. Alternatively, the fob may be placed in a mode as such that the fob account number is provided by USB port 132 (or serial port) only and the fob transponder 114 is disabled. In addition, the term "inclusively" may mean that the fob 102 is placed in an operational mode permitting the fob 102 to be responsive to the RF interrogation and interrogation via the USB connector 132. In one particular embodiment, the switch 230 may remain in an OFF position ensuring that one or more applications or accounts associated with the fob 102 are non-reactive to any commands issued by RFID reader 104. As used herein, the OFF position may be termed the "normal" position of the activation switch 230, although other normal positions are contemplated.

[0051] In another exemplary embodiment, when the switch 230 is moved from the OFF position, the fob 102 may be deemed activated by the user. That is, the switch 230 may activate internal circuitry in fob 102 for permitting the fob to be responsive to RF signals (*e.g.*, commands from RFID reader 104). In this way, switch 230 may facilitate control of the active and inactive states of the fob 102. Such control increases the system security by preventing inadvertent or illegal use of the fob 102.

[0052] In one exemplary embodiment, switch 230 may be a simple mechanical device in communication with circuitry which may electrically prevent the fob from being powered by a RFID reader. That is, when switch 230 is in its normal position, switch 230 may provide a short to the fob 102 internal circuitry, preventing fob 102 from being responsive to interrogation by RF or via the USB connector 230. In this arrangement, the switch 230 may be, for example, a "normally closed" (NC) configured switch, which may be electrically connected to the antenna 202 at the interface of the antenna 202 and the transponder 114. The switch 230 may be depressed, which may open the switch 230 fully activating the antenna 202.

[0053] In yet another exemplary embodiment, the fob 102 may include a biometric sensor and biometric membrane configured to operate as switch 230 and activate the fob 102 when provided biometric signal from the fob 102 user. Such biometric signal may be the digital reading of a fingerprint, thumbprint, or the like. Typically, where biometric circuitry is used, the biometric circuitry may be powered by an internal voltage source (*e.g.*, battery). In this case, the switch may not be a simple mechanical device, but a switch which is powered. In yet another exemplary embodiment, switch 230 may be battery powered though no biometric circuitry is present in the fob 102.

[0054] In yet another embodiment, the switch 230 may be a logic switch. Where switch 230 is a logic switch the switch 230 control software may be read from the sequence controller 208 to selectively control the activation of the various fob 102 components.

[0055] FIG. 3 illustrates an exemplary block diagram of a RFID reader 104 in accordance with an exemplary embodiment of the present invention. RFID reader 104 includes, for example, an antenna 106 coupled to a RF module 302, which is further coupled to a control module 304. In addition, RFID reader 104 may include an antenna 108 positioned remotely from the RFID reader 104 and coupled to RFID reader 104 via a suitable cable 120, or other wire or wireless connection.

[0056] RF module 302 and antenna 106 may be suitably configured to facilitate communication with fob 102. Where fob 102 is formatted to receive a signal at a particular RF frequency, RF module 302 may be configured to provide an interrogation signal at that same frequency. For example, in one exemplary embodiment, fob 102 may be configured to respond to an interrogation signal of about 13.56 MHz. In this case, RFID antenna 106 may be 13 MHz and may be configured to transmit an interrogation signal of about 13.56 MHz. That is, fob 102 may be configured to include a first and second RF module (*e.g.*, transponder)

where the first module may operate using a 134 kHz frequency and the second RF module may operate using a 13.56 MHz frequency. The RFID reader 104 may include two receivers which may operate using the 134 kHz frequency, the 13.56 MHz frequency or both. When the reader 104 is operating at 134 kHz frequency, only operation with the 134 kHz module on the fob 102 may be possible. When the reader 104 is operating at the 13.56 MHz frequency, only operation with the 13.56 MHz module on the fob 102 may be possible. Where the reader 104 supports both a 134 kHz frequency and a 13.56 MHz RF module, the fob 102 may receive both signals from the reader 104. In this case, the fob 102 may be configured to prioritize selection of the one or the other frequency and reject the remaining frequency. Alternatively, the reader 104 may receive signals at both frequencies from the fob upon interrogation. In this case, the reader 104 may be configured to prioritize selection of one or the other frequency and reject the remaining frequency.

[0057] Further, protocol/sequence controller 314 may include an optional feedback function for notifying the user of the status of a particular transaction. For example, the optional feedback may be in the form of an LED, LED screen and/or other visual display which is configured to light up or display a static, scrolling, flashing and/or other message and/or signal to inform the fob 102 user that the transaction is initiated (*e.g.*, fob is being interrogated), the fob is valid (*e.g.*, fob is authenticated), transaction is being processed, (*e.g.*, fob account number is being read by RFID reader) and/or the transaction is accepted or denied (*e.g.*, transaction approved or disapproved). Such an optional feedback may or may not be accompanied by an audible indicator (or may present the audible indicator singly) for informing the fob 102 user of the transaction status. The audible feedback may be a simple tone, multiple tones, musical indicator, and/or voice indicator configured to signify when the fob 102 is being interrogated, the transaction status, or the like.

[0058] RFID antenna 106 may be in communication with a transponder 306 for transmitting an interrogation signal and receiving at least one of an authentication request signal and/or an account data from fob 102. Transponder 306 may be of similar description as transponder 114 of FIG. 2. In particular, transponder 306 may be configured to send and/or receive RF signals in a format compatible with antenna 202 in similar manner as was described with respect to fob transponder 114. For example, where transponder 306 is 13.56 MHz RF rated antenna 202 may be 13.56 MHz compatible. Similarly, where transponder 306 is ISO/IEC 14443 rated, antenna 106 may be ISO/IEC 14443 compatible.

[0059] RF module 302 may include, for example, transponder 306 in communication with authentication circuitry 308 which may be in communication with a secure database 310. Authentication circuitry 308 and database 310 may be of similar description and operation as described with respect to authentication circuitry 210 and secure memory database 214 of FIG. 2. For example, database 310 may store data corresponding to the fob 102 which are authorized to transact business over system 100. Database 310 may additionally store RFID reader 104 identifying information for providing to fob 102 for use in authenticating whether RFID reader 104 is authorized to be provided the fob account number stored on fob database 214.

[0060] Authentication circuitry 308 may be of similar description and operation as authentication circuitry 210. That is, authentication circuitry 308 may be configured to authenticate the signal provided by fob 102 in similar manner that authentication circuitry 210 may be configured to authenticate the signal provided by RFID reader 104. As is described more fully below, fob 102 and RFID reader 104 engage in mutual authentication. In this context, "mutual authentication" may mean that operation of the system 100 may not take place until fob 102 authenticates the

signal from RFID reader 104, and RFID reader 104 authenticates the signal from fob 102.

[0061] FIG. 4 is a flowchart of an exemplary authentication process in accordance with the present invention. The authentication process is depicted as one-sided. That is, the flowchart depicts the process of the RFID reader 104 authenticating the fob 102, although similar steps may be followed in the instance that fob 102 authenticates RFID reader 104.

[0062] As noted, database 214 may store security keys for encrypting or decrypting signals received from RFID reader 104. In an exemplary authentication process, where RFID reader 104 is authenticating fob 102, RFID reader 104 may provide an interrogation signal to fob 102 (step 402). The interrogation signal may include a random code generated by the RFID reader authentication circuit 308, which is provided to the fob 102 and which is encrypted using an unique encryption key corresponding to the fob 102 unique identification code. For example, the protocol/sequence controller 314 may provide a command to activate the authentication circuitry 308. Authentication circuitry 308 may provide from database 310 a fob interrogation signal including a random number as a part of the authentication code generated for each authentication signal. The authentication code may be an alphanumeric code which is recognizable (*e.g.*, readable) by the RFID reader 104 and the fob 102. The authentication code may be provided to the fob 102 via the RFID RF interface 306 and antenna 106 (or alternatively antenna 108).

[0063] Fob 102 receives the interrogation signal (step 404). The interrogation signal including the authorization code may be received at the RF interface 114 via antenna 202. Once the fob 102 is activated, the interrogation signal including the authorization code may be provided to the modulator/demodulator circuit 206 where the signal may be demodulated prior to providing the signal to protocol/sequence

controller 208. Protocol/sequence controller 208 may recognize the interrogation signal as a request for authentication of the fob 102, and provide the authentication code to authentication circuit 210. The fob 102 may then encrypt the authentication code (step 406). In particular, encryption may be done by authentication circuit 210, which may receive the authentication code and encrypt the code prior to providing the encrypted authentication code to protocol/sequence controller 208. Fob 102 may then provide the encrypted authentication code to the RFID reader 104 (step 408). That is, the encrypted authentication code may be provided to the RFID reader 104 via modulator/demodulator circuit 206, RF interface 114 (*e.g.*, transponder 114) and antenna 202.

[0064] RFID reader 104 may then receive the encrypted authentication code and decryption it (step 410). That is, the encrypted authentication code may be received at antenna 106 and RF interface 306 and may be provided to authentication circuit 308. Authentication circuit 308 may be provided a security authentication key (*e.g.*, transponder system decryption key) from database 310. The authentication circuit may use the authentication key to decrypt (*e.g.*, unlock) the encrypted authorization code. The authentication key may be provided to the authentication circuit based on the fob 102 unique identification code. For example, the encrypted authentication code may be provided along with the unique fob 102 identification code. The authentication circuit may receive the fob 102 unique identification code and retrieve from the database 310 a transponder system decryption key correlative to the unique fob 102 identification code for use in decrypting the encrypted authentication code.

[0065] Once the authentication code is decrypted, the decrypted authentication code is compared to the authentication code provided by the RFID reader 104 at step 402 (step 412) to verify its authenticity. If the decrypted authorization code is not readable (*e.g.*, recognizable) by the authentication circuit 308, the fob 102 is

deemed to be unauthorized or not authenticated (*e.g.*, unverified) (step 418) and the operation of system 100 is terminated (step 420). Contrarily, if the decrypted authorization code is recognizable (*e.g.*, verified) by the fob 102, the decrypted authorization code is deemed to be authenticated and the fob 102 is considered authenticated (*e.g.*, verified) (step 414), and the transaction is allowed to proceed (step 416). In one particular embodiment, the proceeding transaction may mean that the fob 102 may authenticate the RFID reader 104, although, it should be apparent that the RFID reader 104 may authenticate the fob 102 prior to the fob 102 authenticating the RFID reader 104.

[0066] It should be noted that in an exemplary verification process, the authorization circuit 308 may determine whether the unlocked authorization code is identical to the authorization code provided in step 402. If the codes are not identical then the fob 102 is not authorized to access system 100. Although, the verification process is described with respect to identicality, identicality is not required. For example, authentication circuit 308 may verify the decrypted code through any protocol, steps, or process for determining whether the decrypted code corresponds to an authorized fob 102.

[0067] Authentication circuitry 308 may additionally be in communication with a protocol/sequence controller 314 of similar operation and description as protocol/sequence controller 208 of FIG. 2. That is, protocol/sequence device controller 314 may be configured to determine the order of operation of the RFID reader 104 components. For example, FIG. 5 illustrates and exemplary decision process under which protocol/sequence controller 314 may operate. Protocol/sequence controller 314 may command the different components of RFID reader 104 based on whether a fob 102 is present (step 502). For example, if a fob 102 is not present, then protocol/sequence controller 314 may command the RFID reader 104 to provide an uninterrupted interrogation signal (step 504). That is, the

protocol/sequence controller may command the authentication circuit 308 to provide an uninterrupted interrogation signal until the presence of a fob 102 is realized. If a fob 102 is present, the protocol/sequence controller 314 may command the RFID reader 104 to authenticate the fob 102 (step 506).

[0068] As noted above, authentication may mean that the protocol/sequence controller 314 may command the authentication circuit 308 to provide fob 102 with an authorization code. If a response is received from fob 102, protocol/sequence controller may determine if the response is a response to the RFID reader 104 provided authentication code, or if the response is a signal requiring authentication (step 508). If the signal requires authentication, then the protocol/sequence controller 314 may activate the authentication circuit as described above (step 506). On the other hand, if the fob 102 signal is a response to the provided authentication code, then the protocol/sequence controller 314 may command the RFID reader 104 to retrieve the appropriate security key for enabling recognition of the signal (step 510). That is, the protocol/sequence controller 314 may command the authentication circuit 308 to retrieve from database 310 a security key (*e.g.*, transponder system decryption key), unlock the signal, and compare the signal to the signal provided by the RFID reader 104 in the authentication process (*e.g.*, step 506). If the signal is recognized, the protocol/sequence controller 314 may determine that the fob 102 is authorized to access the system 100. If the signal is not recognized, then the fob is considered not authorized. In which case, the protocol/sequence controller 314 may command the RFID controller to interrogate for authorized fobs (step 504).

[0069] Once the protocol/sequence controller determines that the fob 102 is authorized (step 512), the protocol/sequence controller 314 may seek to determine if additional signals are being sent by fob 102 (step 514). If no additional signal is provided by fob 102, then the protocol/sequence controller 314 may provide all the

components of RFID reader 104 to remain idle until such time as a signal is provided (step 516). Contrarily, where an additional fob 102 signal is provided, the protocol/sequence controller 314 may determine if the fob 102 is requesting access to the merchant point of sale terminal 110 (*e.g.*, POS device) or if the fob 102 is attempting to interrogate the RFID reader 104 for return (*e.g.*, mutual) authorization (step 518). Where the fob 102 is requesting access to a merchant point of sale terminal 110, the protocol/sequence controller 314 may command the RFID reader to open communications with the point of sale terminal 110 (step 524). In particular, the protocol/sequence controller may command the point of sale terminal communications interface 312 to become active, permitting transfer of data between the RFID reader 104 and the merchant point of sale terminal 110.

[0070] On the other hand, if the protocol/sequence controller determines that the fob 102 signal is a mutual interrogation signal, then the protocol/sequence controller may command the RFID reader 104 to encrypt the signal (step 520). The protocol/sequence controller 314 may command the encryption authentication circuit 318 to retrieve from database 320 the appropriate encryption key in response to the fob 102 mutual interrogation signal. The protocol/sequence controller 314 may then command the RFID reader 104 to provide the encrypted mutual interrogation signal to the fob 102 (step 522). The protocol/sequence controller 314 may command the authentication circuit 318 to provide an encrypted mutual interrogation signal for the fob 102 to mutually authenticate. Fob 102 may then receive the encrypted mutual interrogation signal and retrieve from authentication circuitry 212 a RFID reader decryption key.

[0071] Although an exemplary decision process of protocol/sequence controller 314 is described, it should be understood that a similar decision process may be undertaken by protocol/sequence controller 208 in controlling the components of fob 102. Indeed, as described above, protocol/sequence controller 314 may have

similar operation and design as protocol/sequence controller 208. In addition, to the above, protocol/sequence controllers 208 and 314 may incorporate in the decision process appropriate commands for enabling USB interfaces 222 and 316, when the corresponding device is so connected.

[0072] Encryption/decryption component 318 may be further in communication with a secure account number database 320 which stores the security keys necessary for decrypting the encrypted fob account number. Upon appropriate request from protocol/sequence controller 314, encryption/decryption component (*e.g.*, circuitry 318) may retrieve the appropriate security key, decrypt the fob account number and forward the decrypted account number to protocol sequence controller 314 in any format readable by any later connected POS device 110. In one exemplary embodiment, the account number may be forwarded in a conventional magnetic stripe format compatible with the ISO/IEC 7813 standard. Upon receiving the account number in magnetic stripe format, protocol/sequence controller 314 may forward the account number to POS device 110 via a communications interface 312 and data link 122, as best shown in FIG. 1. POS device 110 may receive the decrypted account number and forward the magnetic stripe formatted account number to a merchant network 112 for processing under the merchant's business as usual standard. In this way, the present invention eliminates the need of a third-party server. Further, where the POS device 110 receives a response from network 112 (*e.g.*, transaction authorized or denied), protocol/sequence controller 314 may provide the network response to the RF module 302 for optically and/or audibly communicating the response to the fob 102 user.

[0073] RFID reader 104 may additionally include a USB interface 316, in communication with the protocol/sequence controller 314. In one embodiment, the USB interface may be a RS22 serial data interface. Alternatively, the RFID reader 104 may include a serial interface such as, for example, a RS232 interface in

communication with the protocol/sequence controller 314. The USB connector 316 may be in communication with a personalization system (not shown) for initializing RFID reader 104 to system 100 application parameters. That is, prior to operation of system 100, RFID reader 104 may be in communication with a personalization system for populating database 310 with a listing of security keys belonging to authorized fobs 102, and for populating database 320 with the security keys to decrypt the fob 102 account numbers placing the account numbers in ISO/IEC 7813 format. In this way, RFID reader 104 may be populated with a unique identifier (*e.g.*, serial number) which may be used by fob authentication circuitry 210 to determine if RFID reader 104 is authorized to receive a fob 102 encrypted account number.

[0074] FIG. 6 illustrates an exemplary flow diagram for the operation of system 100, in accordance with the present invention. The operation may be understood with reference to FIG. 1, which depicts the elements of system 100 which may be used in an exemplary transaction. The process is initiated when a customer desires to present a fob 102 for payment (step 602). Upon presentation of the fob 102, the merchant initiates the RF payment procedure via an RFID reader 104 (step 604). In particular, the RFID reader sends out an interrogation signal to scan for the presence of fob 102 (step 606). The RF signal may be provided via the RFID reader antenna 106 or optionally via an external antenna 108. The customer then may present the fob 102 for payment (step 608) and the fob 102 is activated by the RF interrogation signal provided.

[0075] The fob 102 and the RFID reader 104 may then engage in mutual authentication (step 610). Where the mutual authentication is unsuccessful (step 612), an error message may be provided to the customer via the RFID optical and/or audible indicator (step 614) and the transaction may be aborted (step 616). Where the mutual authentication is successful (step 612), the RFID reader 104 may provide the customer with an appropriate optical and/or audible message (*e.g.*, "transaction

processing" or "wait") (step 618). The fob protocol/sequence controller 208 may then retrieve from database 214 an encrypted fob account number and provide the encrypted account number to the RFID reader 104 (step 620).

[0076] The account number may then be provided to the merchant system 130 for processing. In one exemplary embodiment, the RFID reader 104 may decrypt the account number and convert the account number into magnetic stripe (ISO/IEC 7813) format (step 622) prior to providing the account number to the merchant system 130 (step 628). In particular, the account number may be provided to the POS 110 device for transmission to the merchant network 112 for processing under known business transaction standards. The POS device 110 may then send an optical and/or audible transaction status message to the RFID reader 104 (step 630) for communication to the customer (step 632).

[0077] In another exemplary embodiment, the fob 102 may provide the account number to the merchant system 130 (step 624) in magnetic stripe format, so that the reader 104 does not need to convert the account number to magnetic stripe format. In this embodiment, the account number may or may not be encrypted prior to providing the account number to the merchant system for processing.

[0078] One key concern with providing an unencrypted account number to the merchant system 130 is that the unencrypted account number may be intercepted and later used to complete fraudulent transactions. As such, the present invention employs a proxy account number (*e.g.*, proxy account identifier), which is provided to the merchant system 130 for transaction processing under the merchant business as usual standards (or with minimal changes or customizations). The proxy account identifier according to the present invention may be in similar format as is the account number so that the merchant system 130 is unaware that it is receiving proxy data. For example, if the account number is typically provided to the merchant system 130 in magnetic stripe format, then the proxy account identifier may also be

in magnetic stripe format. It should be noted that the magnetic stripe format is discussed herein by way of example, and the present invention contemplates that the account number and the proxy account identifier may take any form recognizable by the merchant system 130.

[0079] As noted, the account number may ordinarily contain several portions reserved for predetermined information. For example, where the account number is in magnetic stripe format, the account number portions are governed by the International Standards Organization ISO/IEC 7811, et al. standard, which are hereby incorporated by reference. The standard requires the magnetic stripe information to be encoded in three "tracks," *i.e.*, track 1, track 2, and track 3.

[0080] Data stored in track 1 is typically used to verify the user's identity. Track 1 may be reserved for encoding the transaction account identifier, the name of the account holder, and at least the expiration date of the transaction account or the transaction device. The information encoded in track 1 may be alpha-numeric and may be encoded at about 7 Bits/Character. FIG. 7 illustrates an exemplary layout of the data stored in track 1, wherein track 1 is segmented into several distinct predetermined portions (*e.g.*, "fields") for encoding the various account identifying information. The following table may be useful for determining the field definitions of the information provided.

Table of Field Codes for Track 1

SS=Start Sentinel "%"
FC=Format Code
PAN=Primary Acct. # (19 digits max)
FS=Field Separator "^"
Name=26 alphanumeric characters max.
Additional Data=Expiration Date, offset, encrypted PIN, etc.
ES=End Sentinel "?"
LRC=Longitudinal Redundancy Check

Table 1.

[0081] Track 2 is the track most commonly used by the American Banking Association associated banking institutions. Track 2 is typically reserved for a duplicate version of the transaction account identifier and the expiration date of the transaction account or the transaction device stored in track 1. In addition, track 2 may include an encrypted Personal Identification Code, and other discretionary data. However, the data in track 2 is encoded at a lower Bit per Character density than the data encoded in track 1. The data in track 2 may be numeric only and may be encoded at about 5 Bits/Character. The lower density ratio in track 2 is designed to ensure compatibility with older technology readers and to provide redundancy when reading with newer technology readers. FIG. 8 illustrates an exemplary layout of the data stored in track 2, wherein track 2 is segmented into several distinct predetermined portions for encoding the various account identifying information. As shown, the following table may be useful for determining the definitions of the information provided.

Table of Field Codes for Track 2

SS=Start Sentinel "%"
SS=Start Sentinel ";"
PAN=Primary Acct. # (19 digits max)
FS=Field Separator "="
Additional Data=Expiration Date, offset, encrypted PIN, etc.
ES=End Sentinel "?"
LRC=Longitudinal Redundancy Check

Table 2.

[0082] Track 3 is of similar description as Track 2. With the International Standards Organization adoption of standard ISO/IEC 4909, track 3 of the magnetic stripe format was no longer used by the banking industry. However, other transaction devices including a magnetic stripe, such as drivers licenses, use track 3, which may include both numeric only and alpha numeric characters. Track 3 is unique in that track 3 was intended to have data read and WRITTEN on it. Cardholders would

have account information UPDATED right on the magnetic stripe. Unfortunately, track 3 is almost an orphaned standard, since most readers currently in operation are not configured to write data onto a magnetic stripe. The original design of track 3 was to control off-line ATM transactions by recording transaction data for later reference by the banking institution. But since ATMs are now on-line, the usage of track 3 has been drastically reduced.

[0083] The most common technique used to encode data in magnetic stripe format is known as Aiken Biphase, or 'two-frequency coherent-phase encoding.' The American National Standards Institute (ANSI) and the International Standards Organization (ISO) have chosen two standards to guide the encoding process. The ISO encoding protocol specifies that each of tracks 1, 2 and 3 must begin and end with a length of all Zero bits, called CLOCKING BITS. These are used to synch the self-clocking feature of bi-phase decoding. In addition, most transaction devices which use magnetic stripe encoding protocol use either the ANSI/ISO ALPHA Data format or the ANSI/ISO BCD Data format. For example, track 1 is typically encoded in ANSI/ISO ALPHA Data format which is a 7 bit, 6 data bits + 1 parity bit (odd) format, where the data is read least significant bit first. The ANSI/ISO ALPHA format character set contains 64 characters, 43 alphanumeric, 3 framing/field characters and 18 control/special characters. On the other hand, tracks 2 and 3 are typically encoded in ANSI/ISO BCD Data format, which is a 5 bit, 4 data bits + 1 parity bit(odd) format. The character set for the ANSI/ISO BCD Data format character set contains 16 characters, 10 alphanumeric, 3 framing/field characters and 3 control/special characters.

[0084] The present invention takes advantage of the traditional encoding formats in the generation of the proxy transaction account identifier. In general, the proxy transaction account identifier is formatted using similar formatting as is used by the account provider such that the proxy account identifier emulates the account

provider's preferred account identifier format. In the exemplary embodiment described herein, the proxy account identifier may be formatted using the encoding protocol and standards discussed above. The proxy account identifier may be encoded into "proxy tracks" 1, 2 and 3 according to the ISO/IEC 7811 et al. standard. The three separate portions or tracks 1, 2 and 3 are called "proxy tracks" 1, 2 and 3, herein for consistency with magnetic stripe terminology. However, the present invention contemplates that the proxy tracks are further segmented into sub-portions or sub-fields ("proxy fields") which are undetectable (or substantially undetectable) to the reader or the merchant system. For example, the proxy transaction account identifier may include three proxy tracks 1, 2, 3 of the magnetic stripe data which are encoded with a plurality of proxy fields without (or minimally) disturbing the manner in which the proxy tracks are received by the merchant system or reader. Each proxy field may have any field length as determined by the account provider so long as the proxy track containing the proxy fields meets the character bit density of the corresponding magnetic stripe track as defined by the magnetic stripe standard used by the account provider. The proxy fields in accordance with the present invention are shown as PF1- PFn shown in FIGs. 9 and 10.

[0085] Proxy tracks 1, 2, and 3 may be of similar description as traditional magnetic stripe tracks 1, 2, and 3 described above. As such, the information encoded in the proxy tracks ordinarily conforms to the American National Standards Institute and International Standards Organization noted above. That is, proxy tracks may be encoded with data using one of the ANSI/ISO ALPHA Data format or the ANSI/ISO BCD Data format.

[0086] The proxy tracks may be encoded with the relevant transaction account identifying data by the account provider. The encoding is preferably completed prior to populating the proxy account identifier into the fob database 214. The proxy

account identifier may be provided to the fob database 214 prior to providing the fob 102 to an accountholder for usage. Alternatively, the fob 102 may add the proxy account identifier to the fob database 214 at a later date, for example, using the method described in the U.S. Patent Application Serial No. 10/708,550 entitled "SYSTEMS AND METHODS FOR PROVIDING A RF TRANSACTION DEVICE OPERABLE TO STORE MULTIPLE DISTINCT ACCOUNT," which was filed on March 10, 2004, and which is commonly owned by the assignee of the present invention and is hereby incorporated by reference.

[0087] The proxy account identifier is useful for securing the related account identifier, because only subparts or portions of the data sets encoded in the related account identifier are encoded in the proxy account identifier proxy tracks. The portions may be encrypted prior to providing the portions to the proxy track using any method as desired by the account provider. The portions of the account identifier which are encoded in the proxy tracks may be used by the account provider to regenerate the complete corresponding data set, for use in locating the corresponding transaction account for use in transaction completion. In this context, a data set may be groups of information. For example, one data set may be the account number, while anther data set may be the accountholder name, while yet another data set may be the transaction account expiration date, while still another data set may be the transaction account expiration date.

[0088] A more complete understanding of method for encoding the portions of account identifier data into the proxy account identifier may be understood with reference to FIGs. 10, and 11, where FIG. 11 illustrates an exemplary method for encoding proxy account identifier track 1, which may be encoded using the ANSI/ISO ALPHA Data format.

[0089] An exemplary method for encoding the proxy tracks may begin with a customer opening a transaction account with a transaction account provider (step

1102). In opening the account, the customer provides the account provider with personal information such as, for example, the customer's name, street address, city and state. In other embodiments, the fob 102 may include other personal information, such as, for example, the customer's driver's license number, birth date, sex, height, weight, hair color, eye color, or the like.

[0090] Once the information is received, the account provider may open a transaction account and assign the transaction account a transaction account identifier and a transaction account expiration date or effective date (step 1104). The transaction account identifier, effective date, expirations date, and any other information provided by the customer or the account provider, which relates to the transaction account, may be stored on the provider system database such that each piece of information is correlated to the customer transaction account identifier (step 1106).

[0091] Ordinarily, the account provider may provide the customer with an account identifier associated with a transaction device using the information provided by the user and the information from the account provider. The account identifier may be in any format recognizable by the entity receiving the information. For example, where the account identifier is provided to a fob 102, the account identifier is ordinarily received by a reader 104 or merchant system 130. Consequently, the account identifier typically is configured in a format recognizable by the reader 104 or the merchant system 130.

[0092] In a banking context, the account identifier is formatted in accordance with the ANSI/ISO encoding standard. As such, the associated proxy account identifier will also employ the ANSI/ISO encoding standard, except that, as noted, the proxy account identifier only encodes portions of the information data sets that are encoded in the traditional account identifier.

[0093] For example, track 1 of the traditional account identifier is generally reserved for encoding the account number, expiration date and name of the accountholder (*e.g.*, "customer"). That is, the full and complete data set encoded in traditional track 1 may include all characters which comprise a full data set of the traditional track 1 information. However, in accordance with the present invention, the proxy track 1 may only have portions of the traditional track 1 data set encoded in the proxy track 1 location. As noted, FIG. 11 illustrates an exemplary proxy track 1 layout, wherein the proxy fields (PF1-PFN) are shown.

[0094] Where the traditional track 1 may include a field PAN for encoding the transaction account number, proxy track 1 may only encode a predetermined portion of the account number therein (step 1108). The predetermined portion of the account number may be stored in a proxy field such as proxy field PF5. Thus, if the account number is a sixteen-digit credit card account number, the proxy field PF5 may have only the first eight digits of the account number (or any eight digits), thereby freeing up the remaining eight digit positions located in proxy field PF6 for use in storing alternate information. The account provider may then choose to encode any desired alternate information in the remaining digit positions at proxy field PF6 (step 1108). In one example, the account provider may encode authentication tag data, personal security data, customer health or demographic information or the like in proxy field PF6 (step 1112). In similar manner as is discussed with the account number, only portions of the alternate information may be encoded in proxy track 1 at proxy field PF6. Otherwise, the proxy account identifier is populated into the fob database 214.

[0095] The above process of encoding only portions of a data set may be repeated with respect to proxy track 2 and proxy track 3, if required (step 1116). Once the account provider encodes the desired information in the available proxy track character fields, the account provider may populate the proxy account identifier into

a transaction device for use in completing a transaction (step 1114). For example, where fob 102 is the transaction device, the proxy account identifier may be populated on the fob database 214.

[0096] Ordinarily, the proxy account number (*e.g.*, a portion of the transaction account number) includes essential identifying information, such as, for example, any information that is common to the account provider. The common information (also called "common character," herein) may include the account provider routing number, or common source indicator such as the character spaces reserved to indicate the identification of the issuing bank. Thus, where the proxy transaction account identifier corresponds to an American Express account, the proxy transaction account identifier may include the common character number 3, encoded the field location where such common character is ordinarily encoded in traditional magnetic stripe format.

[0097] FIG. 12 illustrates the encoding of which would ordinarily be done by an entity, such as, for example, MasterCard in track 2 format. FIG. 12 shows the encoding of a MasterCard account number 3111 2222 3333 4444 with expiration date 12/99 in traditional track 1 format. Since MasterCard uses the number 3 to identify its transaction accounts, the proxy account identifier will also use the number 3 so that the receiving system (*e.g.*, reader 104 or merchant system 130, or account provider) further recognizes that the proxy account identifier is from a MasterCard transaction device. It should be noted that in this example, the "3" and the "101" may be common characters to all MasterCard transaction accounts.

[0098] FIG. 13 shows the identical account number, 3111 2222 3333 4444, encoded in the proxy account identifier proxy field PF3, which is reserved for account number data. The PF3 may only store the first four digits and the last four digits, or any combination which includes the common character of the issuing institution identifier the number 3. Thus, the remainder of the character locations (designated in PF4 by

"*") for that account number location PAN is left for the account provider to store any information as desired.

[0099] Once the information is encoded in the transaction device (*e.g.*, fob 102), the fob 102 may be presented for transaction completion using any method described herein (step 1120). For example, the merchant system 130 may receive the proxy transaction account identifier from the fob 102 in similar manner as was discussed with reference to completing a transaction in FIG. 6. The merchant system recognizes the proxy transaction account identifier as referenced to a MasterCard account number because of the common number 3 and processes the proxy transaction account identifier under business as usual standards employed for MasterCard accounts.

[00100] Once a merchant transaction request is received at the account provider location, the account provider may decode the proxy transaction account identifier and reassemble the information contained in the proxy fields (step 1122). The account provider may reassemble or reconstruct the information using one or more account provider algorithms. The algorithms may be specific to a particular proxy field, or the algorithm may be operated on the entire proxy transaction account identifier. The reassembled data may be used to reference the corresponding transaction account on the account provider database for use in completing the transaction (step 1124). The account provider may then locate the appropriate corresponding account and satisfy the merchant transaction request under the account provider's business as usual standard (step 1126).

[00101] As such, it can be readily seen that the present invention has the added advantage over the prior art of being able to store more information in the same character spacing than is currently stored in a traditional track 1 field F3. In addition, the information may be transmitted in traditional magnetic stripe format without the

disadvantage of engaging a third party to configure the information in a merchant recognizable format.

[00102] The preceding detailed description of exemplary embodiments of the invention makes reference to the accompanying drawings, which show the exemplary embodiment by way of illustration. While these exemplary embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the spirit and scope of the invention. Thus, the preceding detailed description is presented for purposes of illustration only and not of limitation, and the scope of the invention is defined solely by the appended claims and their legal equivalents when properly read in light of the preceding description. For example, the steps recited in any of the method or process claims may be executed in any order and are not limited to the order presented.